(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
31 January 2002 (31.01.2002)

PCT

(10) International Publication Number
WO 02/09019 A2

(51) International Patent Classification[7]: G06K

(21) International Application Number: PCT/US01/23336

(22) International Filing Date: 24 July 2001 (24.07.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/625,577 25 July 2000 (25.07.2000) US
09/775,934 2 February 2001 (02.02.2001) US

(71) Applicant *(for all designated States except US)*: **DIGIMARC CORPORATION** [US/US]; Suite 100, 19801 S.W. 72nd Avenue, Tualatin, OR 97062 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **PERRY, Burt, W.** [US/US]; 13544 Provincial Hill Way, Lake Oswego, OR 97035 (US). **CARR, J., Scott** [US/US]; 22655 S.W. Grahams Ferry Road, Tualatin, OR 97062 (US).

(74) Agent: **MEYER, Joel, R.**; Digimarc Corporation, Suite 100, 19801 S.W. 72nd Avenue, Tualatin, OR 97062 (US).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: AUTHENTICATION WATERMARKS FOR PRINTED OBJECTS AND RELATED APPLICATIONS

(57) Abstract: The disclosure describes systems for creating and authenticating printed objects using authentication and copy detection watermarks. For example, one verification system includes a watermark decoder and a verification module. The watermark decoder detects a copy detection watermark in a printed object to determine whether the printed object has been reproduced. The verification module processes a message decoded from an authentication watermark on the printed object to authenticate the printed object or bearer of the printed object. The authentication and copy detection watermarks may be implemented as the same or different watermarks. For example, the copy detection watermark may be a fragile watermark that carries the message and that degrades in response to a reproduction operation, such as photocopying or scanning and then re-printing the object. Alternatively, the authentication and copy detection watermarks may be separate watermarks embedded in an image that is printed on the object. The authentication watermark, in some applications, includes an identifier that links the object to a database entry with related information about the object. This related information can be used to check the bearer of the object by comparing it with attributes of the bearer (such as a user ID or photo) or the validity of the object by comparing it with attributes that are visible or machine readable on the object.

WO 02/09019 A2

Authentication Watermarks for Printed Objects and Related Applications

Related Application Data

This patent application is a continuation in part of US Patent Application 09/625,577, entitled Authenticating Objects Using Embedded Data, filed on July 25, 2000 by Scott Carr and Burt Perry, which is hereby incorporated by reference.

The subject matter of the present application is related to that disclosed in US Patent 5,862,260, and in co-pending applications 09/503,881, filed February 14, 2000; which are hereby incorporated by reference.

Technical Field

The invention relates to methods for authenticating objects, and in particular, relates to methods for embedding security data into products, and methods for authenticating these products using the embedded security data.

Background and Summary

Counterfeiting and piracy have a huge economic impact. While numerous product security features have been developed, there remains a demand for cost effective security measures that inhibit counterfeiting and piracy.

Research in the field of steganography (also called "data hiding") offers promising technology for combating counterfeiting and piracy. One form of steganography is referred to in popular literature as digital watermarking. Digital watermarking is a process for modifying a host signal or object to embed a machine-readable code into the host. The host may be modified such that the embedded code is imperceptible or nearly imperceptible to the ordinary observer upon viewing or playback, yet may be detected through an automated detection process.

Most commonly, digital watermarking is applied to media such as images, audio signals, and video signals. However, it may also be applied to other types of

media, including documents (e.g., through subtle line, word or character shifting), software, multi-dimensional graphics models, and surface textures of objects.

The invention relates to methods for authenticating printed objects using digital watermarks embedded in the images on the objects. One aspect of the invention is a system for authenticating a printed object. The system includes a watermark decoder and a verification module. The watermark decoder detects a copy detection watermark in a printed object to determine whether the printed object has been reproduced. The verification module processes a message decoded from an authentication watermark on the printed object to authenticate the printed object or bearer of the printed object. The authentication and copy detection watermarks may be implemented as the same or different watermarks. For example, the copy detection watermark may be a fragile watermark that carries the message and that degrades in response to a reproduction operation, such as photocopying or scanning and then re-printing the object. Alternatively, the authentication and copy detection watermarks may be separate watermarks embedded in an image that is printed on the object. The authentication watermark, in some applications, includes an identifier that links the object to a database entry with related information about the object. This related information can be used to check the bearer of the object by comparing it with attributes of the bearer (such as a user ID or photo) or the validity of the object by comparing it with attributes that are visible or machine readable on the object.

Another aspect of the invention is a system for creating a printed object. The system includes a watermark encoder and communication application. The watermark encoder encodes a watermark in an image to be printed on a printed object. This watermark is used to authenticate the printed object. The communication application obtains an identifier from a database for embedding into a message payload of the watermark. It also provides to the database information to be associated with the identifier.

Further features will become apparent with reference to the following detailed description and accompanying drawings.

Brief Description of the Drawings

Fig. 1 is a flow diagram illustrating a method for embedding an object identifier into an object.

Fig. 2 is a flow diagram illustrating a method for authenticating an object using the embedded object identifier.

Fig. 3 is a diagram of a system architecture for creating and verifying the authenticity of printed objects using digital watermarks for copy detection and authentication.

Detailed Description

Introduction

The following sections describe a system and related methods for authenticating products. While the description illustrates the system with an example of packaged software product, it applies to a variety of types of objects. In this document, the term "product" broadly encompasses physical objects (e.g., goods), and other objects associated with them like packaging, tags, labels, documentation, and media supplied on, by, or with the object. Within this broad product context, the embedding process may encode security data on any of these types of products. To determine whether a product is authentic, the methods and systems described in this document can be used to evaluate security data embedded on the product itself, its packaging, labels, tags, media, etc.

One implementation of these methods and secure products employs a form of steganography referred to as digital watermarking. However, other forms of steganography may be used as well. There are two principal parts of the product authentication architecture: 1) a system for embedding authentication data into the product; and 2) a system for authenticating the product.

Typically, product makers assign unique identifiers, such as product serial numbers, to each product. In the product security systems describe below, an embedder encodes the serial number as a form of machine readable security data into the product or its packaging. This embedded security data is then used to authenticate the product

and/or control unauthorized use. In the case of software products, for example, the embedded security data may be used to ensure that the user is authorized during installation of the software on the user's machine. In the case of financial or access cards (e.g., debit/credit cards, key cards, corporate badges), the embedded security data may be used to activate the card. In the more general case, the embedded security data may be used to check whether a product is authentic by validating a conspicuous product identifier, such as a visible serial number, with one imperceptibly embedded in the product or its packaging. These systems are detailed further below.

Embedding Security Data Into a Product

Fig. 1 is a flow diagram illustrating a method for embedding security data into a product. The maker or distributor of the product assigns a unique identifier, such as a serial number, to the product. The embedding process takes this identifier 20 and transforms it into a form of data for embedding in the product or its packaging. While the identifier need not be modified before embedding it, there are a number of reasons for doing so. One reason is to convert it into a more compact form for embedding. Another reason is to make the embedded data more secure, i.e. more difficult for counterfeiters or pirates to replicate.

Fig. 1 depicts an example of a data conversion method called a hash 22. The hash is a function that converts the identifier into another number. One form of hash is a checksum, but there are many others. One example of a checksum is one that converts a number or set of numbers (e.g., serial number, product code, etc.) into another number using a sequence of prime numbers. A cryptographic hash may be used to generate a new number from which the original identifier is difficult to derive. Whether hashed or not, the data to be embedded is referred to as "security data."

The embedding process embeds the security data into a machine readable code on the product or its packaging (24). In particular, the process steganographically embeds the security data into the machine readable code on the product or on packaging or labels for the product. A steganographic process embeds information on

the product's surface such that is imperceptible or substantially imperceptible upon ordinary inspection, yet readable by machine.

One form of steganography is called digital watermarking. A variety of digital watermarking schemes may be used to embed the watermark onto the print media. Some example watermark encoding and decoding schemes are provided in US Patent 5,862,260, and in co-pending application 09/503,881, filed February 14, 2000.

In digital watermarking of images printed on physical objects, there is a tradeoff between visual perceptibility and survivability of the watermark. In this application, the watermark is embedded so as to be sufficiently robust to survive analog to digital conversion, digital to analog conversion, and possible other forms of corruption, including geometric distortion, additive noise, and compression. The watermark may be encoded by altering the luminance or one or more other color channels of an image printed on the surface of the product. Alternatively, the watermark may be encoded using clear inks that modulate the microtopology of the product's surface or that are readable when exposed to light in non-visible wavelengths, like UV or infrared. Also, the microtopology of the product surface may be altered in the process of creating the product surface so as to embed a watermark. Alternative machine readable codes may be used as well, such as data glyphs, invisible bar codes, etc.

A digital watermark embedding process typically involves several operations. For example, additional data may be appended to the security data, such as synchronization symbols, error detection codes, etc. After adding this data, the security data includes a sequence of symbols for embedding into the product. Additional operations include error correction and other forms of symbol encoding (e.g., convolution codes, turbo codes, BCH codes, Reed Solomon encoding, M sequences, gold sequences, etc.). These operations transform the original message sequence into a message signal. The message signal may then be further replicated and modulated using spread spectrum modulation techniques. For example, the message signal may be spread over a pseudorandom number or set of pseudorandom numbers and repetitively scattered throughout a host signal.

The host signal (sometimes referred to as the cover signal) is the signal in which the embedded data is hidden. This might be an image printed on an object, label or

package, a layer of visible or invisible inks, line art, text, surface topology of an object, etc. The watermark signal may be replicated in several different contiguous or overlapping regions of the host signal. Each instance of the watermark at these regions can be associated with a corresponding imperceptible watermark template, synchronization or orientation signal that enables the decoder to detect the presence of the watermark and determine its orientation parameters such as translation (x, y coordinates of an origin), rotation, scale, shear, differential scale, etc.

To embed the message signal, an embedding function subtly changes the host signal. Digital watermarks usually operate on a digital form of the host signal to create a digital watermarked signal, which is then converted to analog form. However, the digital watermark may also be applied in the analog domain. A variety of embedding functions have been detailed in the literature about digital watermarking. These functions may be additive, multiplicative (adding or multiplying a message signal with the host signal), or some other function, such as a non-linear quantization function. The quantization function embeds a message symbol (e.g., binary or M-ary) by quantizing a sample value or a characteristic of a set of sample values of the host signal to a quantization level associated with the symbol being encoded. To decode the symbol, the watermarked signal is captured and evaluated (e.g., re-quantized) to determine which quantization level a sample or characteristic of a set of samples most closely corresponds to. This quantization level is then mapped to the corresponding symbol.

The embedding functions may be applied to image samples or characteristics in the spatial domain or some transform domain, like Discrete Cosine Transform, Discrete Wavelet Transform, Discrete Fourier Transform, etc.

For enhanced security, various elements of the embedded data may be encrypted. Some or all of the watermark message, including the security data in the message may be encrypted. Various keys used to encode the watermark may be encrypted as well. For example, a key that defines the location of the watermark signal in the host signal may be encrypted. A key used to decode the spread message signal (e.g., a pseudorandom number) may also be encrypted.

In implementations where instances of the watermark signal are repeated in the host signal, a key in the message payload of one instance of a watermark signal may be used to decrypt a message, such as the security data, in other instance of the watermark signal. The key may be included in a message payload by appending the key to the message or combining it with the message using some function such as an XOR, or multiplication operation that combines the key with the message to create a composite message.

Keys used to decode the watermark or its message payload may also be derived from the host signal itself or from another watermark in the host signal.

Digital watermarks provide a low cost, yet secure method of embedding security data into a product or its packaging. The embedding process can be integrated into the process of printing the object or its packaging. For example, for each product, the printing process may be adapted to print an image embedded with the product's identifier or hashed form of it. This process may be integrated in the mass production of a variety of printable objects, like packaging, containers, labels, product documentation, credit cards, etc.

Authenticating A Product Using Embedded Security Data

Fig. 2 is a flow diagram illustrating a process for authenticating a product using embedded security data. The authentication system includes a user interface, scanner and embedded data decoder. In the case where the embedded data is encoded in a digital watermark, the system may be implemented in a personal computer equipped with an imaging device, such as a CCD camera or scanner.

Authentication begins by prompting the user for the product identifier (30). Typically, this identifier is a product serial number in plain view on the product, its packaging or documentation. The user may enter the product number by simply typing it on a keyboard, or using some other user input device (voice recognition, bar code scanner, etc.) In response to receiving the product identifier, the system prompts the user to present the product for scanning (32). The user then scans the product with a sensor device, such as a CCD camera, to capture a product scan.

Next, the system decodes the embedded data from the product scan (34). In the case of security data embedded in digital watermark on the product, the system scans one or more image frames of the product. It then proceeds to detect the watermark in this image signal. Finding a watermark, it decodes the watermark message, including any security data.

To validate the security data (36), the authentication system re-computes the security data from the product identifier entered by the user. It then compares the computed security data with the decoded security data. If the two sets of security data match, then the system deems the product to be valid.

A variety of actions may be triggered by the outcome of the validation process 36. One action is to convey the output of the validation process to the user via a user interface, such as audio output, graphical user interface, etc. This type of operation could be used to authenticate any type of product using an authentication system implemented in a personal computer with an image sensor and software for executing the authentication operations.

In the case of a software product, the validation process (36) can automatically launch installation of the software on the user's computer. A variety of additional post-validation actions may be triggered automatically, such as establishing a connection to another computer (e.g., web server) to facilitate on line registration of the product, downloading of additional software or other content, retrieval of one or more keys that enable the software's operation, etc.

The same actions also apply to other types of products that execute machine instructions from a machine readable memory device. For example, hardware devices with embedded software or firmware could be authenticated in a similar fashion. In particular, the user would enter a product number into a user interface of the device, or another device in communication with it (a nearby PC connected via a wire or wireless port- USB, Firewire, Bluetooth, Infrared link, etc.). The user interface then would prompt the user to scan the product with a camera connected directly to the device being authenticated or indirectly through another device (e.g., the nearby PC). An embedded data decoder would then detect and decode any security data and take actions triggered by the result of the validation process. One action would be to install

software to the device being authenticated from a nearby device or computer network. Another action would be to load one or more keys or other instructions that enable functionality of the device being authenticated.

The application of the authentication system to the registration and installation of software and embedded systems may be extended more generally to many forms of digital content, such as software, music, movies, games, etc. In each of these applications, the authentication method and system is similar. The digital content being authenticated may be packaged on a variety of storage media, such as an optical disk, magnetic disk, flash memory card, etc. The storage media or its packaging (e.g., a DVD case) includes embedded security data that is readable by machine and that is validated against a product identifier. The validation process may trigger actions relating to the digital content stored on the storage medium, such as control rendering of the content, control transfer of the content from the storage medium to another device, control usage of the content (e.g., number of copies, transfers, etc. allowed), linking to a network to retrieve related information or actions (e.g.., linking to a product web site to get more information, license rights or purchase products or services).

The method depicted in Fig. 2 is also applicable to activation of financial and access cards like credit/debit cards, card keys, corporate badges that include keys for accessing buildings, computer systems (including access to a single machine or access to network resources), etc. To illustrate this application, consider an implementation of the authentication system on a network. First, the user receives a new card along with an identifier. This identifier might be one printed conspicuously on the card or given to the user separately (e.g., such as a corporate personnel number). The user enters this identifier and scans the card with an image sensor (e.g., a PC camera, flatbed scanner, etc.) An embedded data decoding process extracts security data, if any, from the scanned image, and validates it against the data entered by the user. If the embedded data is valid, then the authentication system activates the card.

While the system for activating cards can be implemented on a stand alone computer system, it may be more commonly implemented in a network configuration. The system might be implemented in a client server architecture where a client computer at the user's location performs object scanning and decoding functions, and

the server at a remote location validates the embedded data against data supplied by the user. The locations of computer processes that perform the various card activation operations (prompting for user input, scanning, decoding and validation) can be distributed between the client and one or more server computers.

The process of validating a product identifier with embedded security data can be extended in various ways. The embedded data and product identifier entered by the user may be used to form a key to decrypt data supplied in or by the product (e.g., software or multimedia content stored on a CD, DVD, etc.). In this case, the data supplied in or by the product is encrypted and the embedded data is used to convey one element of the key. Other elements of the key may be a product identifier, such as a serial number on the product, and a password of the user. Typically, the data supplied in the product is encrypted by the publisher when the product is made (e.g., burning of a CD, DVD, etc.). However, the encryption and security data embedding processes may be performed whenever data is transferred onto the product (e.g., transfer of data onto a writable storage device).

An additional enhancement is to use the cryptographic key formed from the embedded data and the user entered data (e.g., product identifier, password, etc.) to decrypt yet another key. This additional key can then be used to decrypt content supplied on or by the product. The product may be a storage device such as optical disk, magnetic storage device, flash memory, etc. that carries encrypted data, or some other type of device that supplies encrypted content.

Some examples of such devices are receivers of scrambled content like computers, set-top boxes, personal digital assistants, audio and video players, etc. Consider an example where a user wishes to watch a pay per view movie. The cable provider distributes promotional cards that enable the card holder to access the movie. To access the movie, which is provided in encrypted form via a set-top box or other cable receiver, the user displays the card to a camera connected to the set-top box through a wire or wireless connection. The set-top box decodes embedded security data on the card and combines it with other user and/or product information, such as the user's password, set-top box serial number, card number printed on the card, etc. to form a decryption key that is used to decrypt the movie, which streamed to the set-top

box. A similar approach may be applied to other digital content that is downloaded or streamed in an encrypted form over a network, like the Internet, wireless phone network, cable television network, etc.

The security of the embedded data can be enhanced through the use of copy detection technology. Copy detection technology can be used to detect whether a counterfeiter has made a copy of the object bearing the embedded security data. For example, a counterfeiter might try to circumvent the authentication system by making a high quality copy of the image bearing the embedded security data using a scanner or copy machine, and then printing that image on a counterfeit product or its packaging.

The copy detection technology may be used to embed the security data (e.g., a watermark that is used to detect copying and convey security data) or may be separate from the security data (a separate watermark or other auxiliary data that is used to evince copying). One form of copy detection technology is a digital watermark that is altered in a predictable way when copied with a scanner, copy machine, or other imaging device. Such imaging devices apply a transformation to an image (e.g., an analog to digital sampling, color transformation, etc.) that can be detected by a watermark designed to change in a predictable way to such a transformation.

An example of copy detection technology is a "fragile" watermark. The watermark is called fragile because the strength of the watermark signal in a copy of the watermarked original object is less than the strength in the original object. To detect copying, the embedded data decoder attempts to detect the fragile watermark. If the fragile watermark is not present, or has a measured strength that falls below a threshold, then the decoder deems the object to be an invalid copy. There are a variety of ways to measure strength of a watermark signal. One way is to measure the extent of the correlation between an image of the suspect object and a reference fragile watermark signal.

Rather than using a separate fragile watermark, the authentication system may detect copying based on attributes of the watermark used to carry the embedded data. For example, the watermark may include a synchronization or orientation signal used to detect the presence of the watermark and determine its orientation. Copying of a

watermarked object may be detected by measuring changes in the watermark orientation signal.

Since the watermark carrying the embedded data is made to survive distortion due to normal scanning operations required to read the watermark from an object, a fragile watermark may not accurately discern copying by a counterfeiter from these normal transformations. However, the watermark payload may be embedded in ways that survive these normal operations, yet still carries information from which copying can be discerned. For example, the payload of the watermark may be robustly encoded to withstand transformations due to scanning, geometric distortion, etc., yet convey information from which copying can be discerned.

One type of copy detection payload is an identifier that is related to some other characteristic of the object (another machine readable code, like a bar code, magnetic stripe, hologram, etc.).

Another form of copy detection is to scramble or encrypt part or all of the watermark payload in a predictable, yet different manner from one product to the next. This may be accomplished using a cryptographic hash that scrambles the payload using the product number or some other product specific attribute as a seed.

Another way is to scramble the location of the watermark or the relationship between different parts of the watermark using a cryptographic function. For example, the watermark may be replicated in blocks of an image, where each block encodes a similar payload, yet encodes that payload in a different manner based on a secret key. Each block may include an orientation signal that enables the decoder to properly align the image data for that block. In each block, the watermark payload may be scrambled differently, such as using a seed for a cryptographic scrambling function based on block location, block number, or data from the payload of another block, etc.

While the decoding process can use the orientation signal to align each block, it may not be able to discern the precise alignment of blocks in the scanned image relative to blocks in the original watermarked image. As such, the decoder may only be able to recover the relative location of blocks to each other, but not their absolute location in the original image. To address this challenge, the variation of the watermark or its payload across the image can be made in a relative manner from one block to the next

using a secret key that defines the relationship between blocks. Relative changes between neighboring blocks enable the decoder to extract the payload from one block using information from one or more neighboring blocks. For example, the payload of one block may be altered using the payload of one or more adjacent blocks. The relationship between the payloads of adjacent blocks may be defined according to a cryptographic function. For example, the payload of one block may be used as a key to decoding an adjacent block.

A related enhancement is to use keys for decoding the watermark, the watermark payload, or digital content that are dependent on the host signal. This type of host signal dependent key makes it difficult to copy the embedded security data from one object to another. To illustrate this enhancement, consider embedded security data in an image watermark on a product, packaging, or label. One form of image dependent key is a key that is derived from a property of the image that is insensitive to the changes due to the watermark embedding process and recoverable in a watermark decoding operation on the embedded product.

An example of this type of key is a number that is derived from statistical properties of the image that are insensitive to the watermark embedding process, like the relative power differences between blocks of the image. The key could be, for instance, a binary number computed by comparing the power of a given block with a set of other blocks, such as those in a predetermined neighborhood around the given block. The comparison operations yield a one or zero depending on whether the power of the given block is greater or less than the selected neighbors. Each comparison operation yields a single bit in the key. The key may then be appended or combined with the watermark payload.

At the time of authentication, the watermark decoding process employs a synchronization or orientation signal to align the image data. Then it re-computes the image dependent key by repeating the key derivation operation as computed in the embedding process. The key computed at the time of decoding may be compared with the embedded key to check authenticity of the embedded data. Other properties that are insensitive to the watermark process may be used as well.

Another enhancement that can be used as a form of authentication and copy detection is to embed two or more different watermarks that have a known relationship with respect to each other. One such relationship is a predetermined offset in the spatial image domain, or some other transform domain, like a Discrete Fourier Transform, Discrete Cosine Transform, Discrete Wavelet Transform, or some re-sampling of one of these domains, like a log, log-log, or log-polar re-sampling. This known relationship changes in a predictable way when the watermarked object is copied. Thus, during the authentication process, a watermark decoding process detects the watermarks and computes this relationship between the watermarks. It then compares the computed relationship with the known relationship to determine whether some unauthorized transform likely occurred, such as copying.

One way to detect that a detect whether a printed object (e.g., a document, label, ticket, box) has been copied is to embed two watermark signals with different characteristics that change differently in response to reproduction operations such as photocopying, or digital scanning and re-printing. To differentiate a copy from an original, the watermark decoder measures the characteristics of both watermarks in a digital image scan of the printed object, and detects a copy by the changes in the watermarks attributable to reproduction operations. Examples of this approach are described in US Patent Application 09/433,104, entitled Methods and Systems Using Multiple Watermarks, by Geoff Rhoads and Ammon Gustafson, which is hereby incorporated by reference. Four approaches are listed in this document, including :

1. high and low spatial resolution watermarks;

2. one watermark with a geometrically linear assignment of pixels and another with a random assignment of pixels;

3. low and high power watermarks; and

4. one watermark with standard a RGB to HSI – HSI to RGB transform and a second watermark that is biased before being transformed from HSI to RGB.

In the first case, the high resolution watermark is degraded more than the low resolution watermark. The watermark detector detects copying by measuring the change in the power ratio between the two watermarks in a suspect image relative to the original ratio, which is set at embedding and provided to the detector. In the other

cases, the detector detects copying by observing changes in the relative strengths of the detected watermark signals with respect to the original relationship between the watermarks.

Similar techniques may be used to create a fragile watermark that evidences copying due to changes in the fragile watermark's strength relative to its original strength in the un-manipulated original printed object. Also, the fragile watermarks may be adapted to carry a message payload. Finally, the fragile watermarks may be spatially replicated in contiguous blocks of the image. The detector can then isolate the spatial location of blocks of the image where the fragile watermark or watermarks evidence tampering.

The above sections refer to encryption and decryption operations. A variety of cryptographic technologies may be used to implement these operations. Some examples of encryption technologies include RSA, DES, IDEA (International Data Encryption Algorithm), skipjack, discrete log systems (e.g., El Gamal Cipher), elliptic curve systems, cellular automata, etc.

The above sections also refer to hash operations and in some cases, cryptographic hashes. Cryptographic hashes are functions used to convert a first number into a relatively unique second number in a manner that makes it difficult to derive the first number from the second number. Examples of hashing functions include MD5, MD2, SHA, SHA1.

Watermark Embedding and Decoding System

Fig. 3 is a diagram illustrating a architecture for watermark embedding and decoding for printed objects. As described further below, this architecture applies to a variety of printed object types and application scenarios. Before discussing the various object types and applications, this section begins with a description of the system architecture. The implementer may adapt the system for a particular application using one more components of the architecture. Later sections describe a number of example application scenarios based on this architecture.

There are three primary components to the system: 1. a watermark embedding system (40-44) that embeds a digital watermark into an image and prints the

watermarked image on an object 45 (e.g., document, card, label, tag, coupon, ticket, pass, security, certificate of authentication, etc.); 2. a watermark decoding and verification system that reads the watermark from a potentially manipulated version of the printed object 46 and verifies its authenticity (48-56); and a database system (60-70) that performs a variety of functions, depending on the application. These database functions include managing information embedded in the printed objects (e.g., identifiers), managing electronic transactions associated with assigning identifiers and using them in the printed objects, assisting in verification of the printed objects, and maintaining event logs and reports of object usage.

In Fig. 3, these three primary components are interconnected via a network 72 such as the Internet. However, the database functions can be built into the embedder and decoding systems to perform data management and data look up operations locally within those systems.

The embedding and decoding systems are implemented as software applications for an open hardware platform or as special purpose systems. Examples of an open platform implementation include a software application for an operating system like Microsoft Windows or Linux that end-user's install on a computing device with a connection to a network and printer (for embedding) or scanner or digital camera (for decoding and verification). Examples of a special purpose platform include a combined software and hardware system with a network connection (possibly a private network) and a special purpose printer for printing value documents, like boarding passes, tickets, coupons, financial or phone cards, etc. Both the embedding and decoding systems may be implemented in kiosk for public places like coffee shops, restaurants, airports, train stations, bus stations, etc. Such systems can be used for the printing of tickets, passes, coupons, etc., as well as in check in stations for tickets and passes or redemption stations for coupons.

Implemented as a software program or a combination of hardware and software, the embedder application 42 takes an image for printing on an object and embeds a digital watermark in the image comprising an array of sample values (halftone dots or multilevel per pixel samples). Preferably, the digital watermark is substantially imperceptible to a viewer of the image, but that is not a requirement in all

applications. The embedder embeds a message payload into blocks of pixels of an image. Depending on the size of the image and the payload, the message payload may be replicated throughout the image several times to increase robustness. In certain applications, the embedder embeds an identifier into the message payload that is uniquely associated with a printed object or set of similar printed objects. This identifier may be used to identify the object, to link the printed object with information about it stored in a local or remote database, to act as a unit of value or link to a monetary value associated with the object (e.g., a ticket, a piece of postage, a pass, a coupon, etc.), to authenticate the object, to track the usage of the printed object (e.g., to monitor usage of a train or bus pass, to monitor redemption of coupons), etc.

The embedder may also embed into the watermark payload attributes of the image printed on the object, such as a perceptual hash of the image. In addition, it may embed attributes of the bearer of the object such as name, user ID number, age, etc. or other information into the watermark message payload. Also, it may embed text data that is printed on the object (like a document ID, etc.) into the watermark payload. In each case, the embedder may embed text or numeric data representing the attributes themselves, a hash of this data, or a losslessly compressed version of this data.

Additionally, the watermark payload may include a time stamp or a link to a time stamp in the database. This time stamp is useful in verification operations to check the age of the printed object, and process the object according to its age. In some applications, like passes, tickets, debit cards, etc. the printed object becomes invalid and inoperable after a certain period elapses.

For verification, the decoding system derives these attributes from the printed object and compares them with the information in the watermark payload or in the database, which is referenced by the identifier in the watermark payload. A verification module performs the process of verifying authentication attributes derived from the object and elsewhere (e.g., from the database, from the user, etc.). This module may be located in the decoding system, a remote database, or distributed in both systems.

The watermark protocol defines the nature of the watermark signal and its payload. For example, the protocol specifies keys used to encode and decode the watermark, symbol coding schemes like error correction coding, M sequences and gold

sequences, error detection schemes (convolution codes, Reed Solomon codes, BCH codes, etc.), spread spectrum modulation and associated spreading keys, synchronization codes, etc. The protocol may vary from one application to the next. The protocol may define a single robust watermark, a single fragile watermark, or some combination of fragile and robust watermarks. For example, the object may have a single fragile watermark (per image block). This fragile watermark may carry a payload, or simply act as a copy detection watermark that degrades when the printed object is reproduced in a photocopy machine or by scanning and re-printing. The object may have a single robust watermark (per image block) that carries a message payload. Alternatively, the object may include a robust watermark for carrying a message payload, and a fragile watermark that acts as a copy detection watermark. The robust and fragile watermarks may each be implemented as two or more different watermark signals. Also, the watermark signals may include attributes, such as a template, calibration signal or other characteristic features or patterns that are used to correct for geometric distortion in capturing an image of the object for watermark decoding. In some applications, it is useful to ascertain which portions of the object have been tampered with. One way to do this is to repeat a fragile watermark in spatial blocks of the image printed on the object. Then, in the decoding process, a watermark detector indicates which blocks have a detectable fragile watermark and which do not. Another approach is to embed a fragile watermark with a different message payload in each block. Then, in the decoding process the detector reports all of the fragile watermark payloads that it has successfully recovered. The missing payloads indicate the blocks that have been tampered with.

After embedding the watermark in the image, the embedder passes the watermarked image to the printer 44, which in turn, prints the image on an object to create the printed object 45. The watermark survives the transformation from a digital image to a physical printed object, and is typically spread over surface of the object (e.g., repeated in contiguous rectangular blocks throughout the object), which may carry other information, such as the host image in which the watermark is embedded as well as other markings and text. This object undergoes typical or malicious manipulation, such as wear and tear, soiling, crumpling, photocopying, scanning and

re-printing, etc. To depict this manipulation, Fig. 3 graphically depicts the printed object 45 being transformed into a potentially altered version of the object 46 after manipulation.

The watermark decoding system includes an image capture device 48, watermark decoder application 50, and user input/output devices (like a keyboard, display, etc.). It may also include a machine reader 56 to read other machine readable codes from the object (2D or 1D bar code, a magnetic stripe, an RF tag, an integrated circuit chip carrying data about the object, organic transistor, etc.). The information conveyed in these other machine readable codes may be related to the information conveyed in the watermark payload (e.g., through a predetermined mathematical relationship such as one being the hash of the other) for authenticating the printed object.

The watermark decoder employs watermark detecting and reading technology described and referenced in this document to detect a fragile watermark if present, and to read the watermark payload if present. For more on watermark embedding, detecting and reading operations, see U.S. Patent 5,862,260 and US Application 09/503,881, which is incorporated by reference. Depending on the implementation, the watermark decoder may perform one or more verification processes such as: checking for the presence of a fragile watermark or watermarks, measuring the strength of the watermark signal, or comparing the payload information with other verification information entered by the user, read automatically from other machine readable features on the document, printed on the face of the document or fetched from a database, etc. The decoder may also communicate watermark payload information to the database, or use the watermark payload information to look up additional authentication information in the database via a network connection.

The watermark detection and/or payload reading of one or more watermarks in the image may be based on user provided key information, such as a password, which may be combined with an image hash or other information on the object to provide a watermark detection key (e.g., a pseudorandom pattern) or a watermark payload descrambling or decoding key.

As detailed further below, the watermark may also link the printed object to a database entry storing information about the user. The decoding system or database compares the user information in the database entry with that supplied by the user to verify that the printed object is being presented for verification by the proper user. This feature is useful to verify that certain types of items, like tickets, boarding passes, legal documents, etc. are not only authentic but also are being presented by the appropriate person. This user specific information is associated with the identifier embedded in the printed object by the embedding system, which communicates the association between the ID and the specific user to the database at the time of embedding.

As shown in Fig. 3, both the embedding and decoding systems may take advantage of a database for a variety of functions. This database may be local or remote as shown in Fig. 3. The embedding and decoding systems shown in Fig. 3 include a communication application (40, 54, respectively). This application enables the systems to communicate with the database system via a network. For the typical implementation adapted for computer networks like the Internet, this communication application represents network communication software and network interface hardware to connect computers on a network. For example, the communication application implements a TCP/IP protocol, and uses standard communication technologies like SSL, HTTP, and XML to pass information. The specific connections can be made over a public or private network, WAN, or LAN. Both the embedding and decoding system can be designed to be portable or fixed at one location, either with a connection to the network that is always on or that is established on demand.

The database in Fig. 3 communicates with the embedding and decoding systems via a compatible communication application 60. For example, an application adapted for the internet uses standard Internet communication protocols, and if security is desired, a secure connection like SSL. As shown, the database may also communicate with the other remote systems through a firewall that restricts communication to messages from authenticated machines and/or users. To authenticate a machine, the firewall only allows message packets from machines with a particular machine address (e.g., a particular set or class of IP addresses). To authenticate individual users of the

embedding and decoding systems, the firewall requires the user to enter the appropriate password and log-in information. For some applications, the database may be public, in which case, these security measures are not necessary.

Behind the firewall, a database management system 64 manages requests for embedding transactions and verification transactions. For certain applications, it maintains an ID database 66 of identifiers (IDs). These identifiers are embedded in the watermark payload of printed objects and used to link back to a database entry for verification or other functions (like linking to a web page or e-commerce transaction, etc.).

The embedding system gets IDs for embedding either in blocks or on demand from the ID database via the database management system. The embedding system, for example, may request a block of IDs for later embedding into watermarked images to be printed on objects. Alternatively, the embedding system may request IDs as needed in a real time connection with the database. In some applications, the database management system implements an electronic transaction to charge a customer's account for each ID or block of IDs that have been requested or registered with that customer. The transaction is associated with the customer via a secure transaction involving customer authentication via a password, and machine authentication via a particular machine address or signature supplied by the embedding computer or printer.

The database entry may include information to verify the authenticity of the printed object, such as features of the document that can be compared with the document to check for authenticity (such as a document number, a machine readable code on the document, a hash of text on the document, a hash of perceptual image features of the document image, etc.). The database may also include information to verify the authenticity of the bearer of the printed objects, such as a special user password or user ID, a picture of the user, or other biometric data of the user (hand writing signature, iris or retinal scan, fingerprint, voice signature, key stroke signature, etc.). This information is captured from the user or embedding system at the time of embedding and added to another database called the ID-Object association database 68.

In particular, the embedding application records the IDs along with the related object and/or user authentication information at the time that the IDs are embedded into

the printed objects. If the embedder application maintains a real-time connection with the database, it transfers the ID along with the associated authentication information back to the database management system 64, which in turn, creates a database record in the ID-object association database 68. The embedder application may also implement a store and forward approach, where it records the ID-authentication information associations, and forwards them to the database when a connection is available.

The embedding system may also associate additional information with printed objects. For example, the customer may want to associate a particular web site address with a printed object so that the printed object is dynamically linked to the web site by the decoding application in conjunction with a look up operation in the ID object association database. For example, in one application for sports tickets, the bearer of the ticket shows the ticked to a web camera connected to a computer enabled with watermark decoding software. The watermark decoder application transmits the ID extracted from the watermarked image on the ticket to the database management system, which in turn, looks up the web site address in the ID-object association database 68 indexed by the ID number. The database management system then returns the web site address to the user's computer, which launches a web browser and fetches the web page at the supplied web address.

For some applications, the database management system is configured to have a public and private side. The public side is used to link watermarked objects to related information, by returning the related information just like the web address in the previous paragraph. The private side is used for authentication operations, such as checking whether a printed object is authentic, checking whether the bearer of the printed object is valid, etc.

In addition to linking to authentication information, the identifiers may also serve the function of representing units of value associated with the printed object. For example, the printed object may be a pass for a bus, train, ski lift, etc. At embedding, the embedding system associates the number of units of value to be associated with the printed object, and charges the buyer's account (electronically debits the buyer's account by the units of value associated with the printed object). At the decoding side, the decoder application 50 extracts an embedded identifier from the watermark in

the image on the object, and connects to the database to determine the amount of value associated with the identifier in the database. The database management system decrements the number of units remaining for the object with each use of the watermarked object. When the number of units remaining drops to zero, the database management system sends back a control signal indicating that the watermarked object is no longer valid.

One variation to this approach is to program the database management system to return control signals to the decoding system for display to the user. In this variation, the control signals warn the user that the number of units remaining has dropped below a threshold, and offer the user the opportunity to buy more units via a secure electronic transaction over the network, such as a credit card transaction. When the user buys more units and refreshes the object in this manner, the database management system increments the number of units associated with the printed object.

The database further includes a customer database 70 to maintain customer account information, such as customer passwords for user authentication and financial transaction information associated with the purchase of identifiers associated with embedding transactions.

In some system designs, the design requirements dictate that the database management system act as a router to other secure databases controlled by different entities. For example, a number of different customers may wish to maintain their own authentication databases, and databases for controlling use of the printed objects under their control. In this case, the database management system 64 uses one or more layers of indirection to link the customer's database to the decoder application 50. In particular, the ID-object association database 68 stores a relationship between an ID and a customer system (e.g., the network address of the computer system controlled by the customer). For authentication or other actions triggered by the ID in the watermark, the database management system 64 looks up the customer's computer address in the database 68 using the ID from the watermark, and either forwards the ID to the customer's database system using the computer address of that system, or returns the customer address information to the decoding system, which in turn establishes a secure connection with the customer database. In the first case, the database

management system also forwards a computer address of the decoding system to the customer database (e.g., the IP address) so that it can respond directly to the decoder application 50 running in the decoding system.

Using this approach, the database management system can act as a router to send transaction requests to many different customer databases in response to decoding a watermark payload. Some objects may even be associated with more than one customer. For example, when a user presents a ticket for verification, the decoding system sends the ID extracted from the watermark to the database management system 64, which in turn, forwards it to the ticketing agent's computer for authentication. The database management system may also link the decoding system to another party's computer, such as the ticket promoter's web site for more information (e.g., promotional information, information about the ticket, electronic commerce opportunities to buy more tickets or related products or services, etc.)

As noted previously, the decoding system does not require a connection to a local or remote authentication database to authenticate the printed object. In some cases, the object can be authenticated by checking the strength or for the presence of a fragile watermark signal. Also, the watermark payload can be designed to carry authentication information like a hash of the watermarked image on the object. To authenticate the image, the hash is decoded from the watermark and compared with a new hash computed of the image of the object (optionally realigned to correct for geometric distortion relative to the orientation, scale and position of the image data when the embedded hash was computed). The sensitivity of the hash to changes can be tuned to detect modifications due to photocopying, scanning, or re-printing. Preferably, the hash is computed of features of the image, such as energy or power at selected spatial frequencies or certain color attributes that degrade predictably in response to photocopying or printing operations. Such an image hash may allow benign image editing like brightness or contrast changes, but detects content additions or deletions to the image. Geometric distortion introduced by copying may also be detected by observing aspect ratio changes of certain visible or hidden fiducials printed in the image.

Another form of authentication is to use certain image features, text content on the printed object, or information provided by the user (such as password, user ID, or other user specific information) as a key to create a watermark pattern (e.g., as a key to a PN number generator that is used to create a noise image that is adapted to the image and added to it). At authentication time, the information used to create the key is obtained from the object, the user, the authentication database, or a combination of these sources. The decoding system then creates the watermark signal from the key, and if the watermark is present, the printed object is authentic. If it is not present, the printed object is deemed not authentic.

Example Applications

The following sections describe how the system may be adapted for a variety of types of printed objects. In each of these cases, copy detection technology, such as fragile watermarks, authentication hashes embedded in the watermark, or special authentication keys used to create the watermark may be used to authenticate the printed object. In addition, the watermark may carry information that is used to access and index information in a database or on a computer network as described above.

Stocks and Bonds

The system shown in Fig. 3 can be used to create print stock certificates and bonds with copy detection watermarks to verify their authenticity. In addition, decoding systems can use the identifier embedded into the watermarks on the documents to link to the database, where information for authenticating the document and/or its owner are stored. As title changes, the database can be updated to associated the current owner and other transaction information with the identifier embedded in the document. Also, the database management system can keep a log of when, where, and by whom the document is presented for authentication and generate detailed reports providing such transaction information.

Visas and Passports

The system can be used to implement similar functions for visas and passports. In particular, the database can be used to store information about the bearer of the visa

or passport, such as a photo, unique user identifier or other information. In the verification process, the decoder extracts the information from the watermark and compares it with authentication information elsewhere in the document or in the database. If the information does not match, then the passport or its bearer are not valid.

For database applications, the passport may be linked to a unique database entry via an identifier embedded in the watermark. For example, border control personnel can compare a photo returned from the database with the person bearing the document to authenticate the bearer of the passport.

Legal Documents

The system can be used to verify and manage legal documents, such as contracts, deeds, title, etc. In addition to providing an authentication function, the watermark can link to a database for additional information about the document in the database via the identifier in the watermark payload. This information may include contact information for the parties of the contract, version control information to indicate whether the contract is the most current and valid document in a series of related documents, information for authenticating that a contract document has been fully executed by all parties, etc.

Insurance Policy

The system can be used for similar functions for insurance policies. In addition, important text information, such as the nature of the insured property, can be stored in a secure database that can be accessed via the identifier embedded in the watermark. If the watermark is unreadable, the insurance policy has been tampered with and is not authentic. If the watermark is readable, but the content on the document has been changed, then the text information in the secure database can be checked by indexing it using the identifier in the watermark payload. This text can then be matched with the text on the document to verify its accuracy. Alternatively, a hash of the text can be embedded in the watermark payload, and compared with a hash of the text on the document to give the document another self authenticating feature.

Purchase orders, Purchase requisitions, Invoices, Bills

The system can be used to authenticate purchase orders, purchase requisition and invoices. In addition, the watermark payload can index information about the purchase order/requisition or invoice in the system's database. The database can provide a variety of information, including financial information regarding the status of the transaction that is dynamically updated as the document is processed. The database returns information for display, such as the transaction status: pending, fulfilled, shipped, shipping date, paid, balance overdue, goods returned, etc. The decoding stations can be used to update the status in the database by sending status updates to it as the document is processed.

Bank statements, Credit card statements

The system provides an effective way to authenticate bank and credit card statements. In addition, the identifier extracted from the watermark on the statement links to personal financial records, account information, etc. stored in the database. This enables the user to show the statement to a digital camera or scanner in a decoding system, and link automatically to related financial records, and account status information. Special user information provided by the user or embedded in the watermark can be used to generate an access code to get access to the database records.

Transportation Tickets

The system can be used to print and authenticate a variety of transportation passes and tickets, such as a single use and multiuse bus or train ticket, an airline ticket and airline boarding pass. The copy detection watermark, in these applications, is used to authenticate the pass. In addition, the watermark payload may be used to authenticate the user as well. For example, the user enters a code at a check-in or verification terminal. This terminal then compares the code with information in the watermark payload, or information linked to the pass via the watermark on the pass. If the user information entered by the user matches the authentication information on the card or in the database linked by the watermark, then the terminal deems the user to be valid. The user information in the watermark payload or database may be related to the

information supplied by the user via a cryptographic function such as a cryptographic hash.

In addition, the pass may be associated with some number of passes or rides via the identifier embedded in the watermark. Each time the pass is used, the watermark is decoded and the corresponding number of passes linked to the object via the watermark is decremented. The identifier in the watermark links the object to a database that stores information about the object, including the number of passes available.

Event Tickets

The system can be used to authenticate event tickets and the users of those tickets as described above. In addition, the watermark can be used to link to additional information about the event that is general or specific to the particular ticket. For example in one application, the database returns images showing how to get to the seat and what the view is from the seat of the event.

Birth Certificates

The system can be used to authenticate birth certificates, as well as link to records in a database relating to the birth certificate, such as when and where the certificate was issued, and procedures for ordering additional copies, etc.

Diploma

The system can be used to authenticate diplomas and other similar items like a certificate of mastery from a class, professional licenses (contractor, doctor, lawyer), etc. In addition, the system can be used to authenticate the bearer of the document to verify that the person presenting the document is its valid owner.

Permits

The system can be used to authenticate permit documents like building permits and inspection permits. In addition, the watermark may also carry an identifier that links the permit to a records database for more information about the project to which the permit relates.

Timesheets

The system can be used to authenticate time sheets and link to an accounting database for related information about a particular project to which the timesheet relates.

Personal Cards

The system may be used to create and verify a variety of types of personal cards, like voter registration cards, library cards, phone cards, financial cards, insurance cards, photo IDs, and other membership cards (health club, etc.). The decoding system can also be used to control access to certain places or things. For example, the system could verify a voter card as well as the voter at a voting booth. In addition, the system maybe used to keep a record of the vote to prevent the voter from voting more than once.

The watermark on the library card could also be used to link the user to a database of book check in/check out transactions and provide information about when items are due.

Product Labels

As detailed above, the system can be used in product security applications to authenticate clothing and merchandise labels, tags, certificates of authenticity, etc. In addition, the watermark can including an identifier that links to a database entry or web site that has product information, warranty information, user instructions, options to purchase related items and accessories, etc.

Using watermarks for product security and links to information applies to product packaging and the products themselves. It can be used on a variety of products, including music CDs, software CDs (both the cover and the physical item), VHS cassettes (both the sleeve and label), DVD ROM (both the cover and the physical item), certificates of authenticity for software, tags for popular items for trading, like Beanie Babies toys, or other merchandise, etc.

Forensic photographs

Fragile digital watermarks can be used to check whether a digital image has been tampered with. However, such applications may not extend to cases where such photographs are printed and kept in a physical file. The system described above can be used to embed authentication watermarks in such images before they are printed. The authentication watermark can be used to authenticate the printed image and also link to a database where a pristine digital copy of the image is stored securely. This applies to prints of insurance photos taken digitally, prints of evidentiary photos (crime scene, etc.), and a variety of other applications.

Concluding Remarks

Having described and illustrated the principles of the technology with reference to specific implementations, it will be recognized that the technology can be implemented in many other, different, forms. To provide a comprehensive disclosure without unduly lengthening the specification, applicants incorporate by reference the patents and patent applications referenced above.

The methods, processes, and systems described above may be implemented in hardware, software or a combination of hardware and software. For example, the auxiliary data encoding processes may be implemented in a programmable computer or a special purpose digital circuit. Similarly, auxiliary data decoding may be implemented in software, firmware, hardware, or combinations of software, firmware and hardware. The methods and processes described above may be implemented in programs executed from a system's memory (a computer readable medium, such as an electronic, optical or magnetic storage device).

The particular combinations of elements and features in the above-detailed embodiments are exemplary only; the interchanging and substitution of these teachings with other teachings in this and the incorporated-by-reference patents/applications are also contemplated.

I claim:

1. A method for authenticating a product comprising:

receiving a product identifier associated with the product;

decoding security data steganographically embedded into the product; and

validating the product by comparing the decoded security data with the product identifier.

2. The method of claim 1 wherein the security data is embedded in a digital watermark that decoded from an image scanned of the product.

3. The method of claim 1 wherein the security data is decoded from a scan of product packaging for the product.

4. The method of claim 1 wherein the product comprises software and including:

controlling installation of software in response to validating the product.

5. The method of claim 1 wherein the product comprises a financial or access card and including:

controlling activation of the card in response to validating the product.

6. The method of claim 1 including:

prompting a user to enter the product identifier; and

prompting the user to scan the product to capture a scan of the embedded security data.

7. The method of claim 1 wherein the embedded security data comprises a hash of the product identifier.

8. The method of claim 1 wherein a copy detection feature included on the product; and further including:

using the copy detection feature to determine whether the product has been counterfeited.

9. The method of claim 8 wherein the copy detection feature comprises a watermark that changes when copied in a manner that enables copying of the product to be detected.

10. The method of claim 8 wherein the copy detection feature comprises a watermark from which copying is detectable from analysis of a payload of the watermark.

11. A computer readable medium having software for performing the method of claim 1.

12. A product including:

security data steganographically embedded into the product; the product being assigned a product identifier that is related to the security data such that authenticity of the product is evaluated by comparing the security data decoded from the product with the product identifier.

13. A method of making a product comprising:

assigning a product identifier to the product;

steganographically embedding security data into the product, the security data including the product identifier; wherein the security data is machine readable and enables automated authentication of the product by comparing the security data decoded from the product with the product identifier.

14. A system for authenticating a printed object comprising:

a watermark decoder for detecting a copy detection watermark in a printed object to determine whether the printed object has been reproduced; and

a verification module for processing a message decoded from an authentication watermark on the printed object to authenticate the printed object or bearer of the printed object.

15. The system of claim 14 wherein the message comprises an identifier that is used to look up authentication information in a database, and including:

a communication application for communicating the identifier to the database to fetch the authentication information associated with the printed object and to provide the authentication information to the verification module.

16. The system of claim 15 wherein the verification module compares authentication information from the database with authentication information provided by the bearer of the printed object to authenticate the bearer of the printed object or the printed object.

17. The system of claim 15 wherein the verification module compares authentication information from the database with authentication information read from a machine readable code on the object to authenticate the object.

18. The system of claim 15 wherein the verification module compares authentication information from the database with authentication information derived from a hash of information on the object.

19. The system of claim 18 wherein the hash is computed of an image on the object.

20. The system of claim 18 wherein the hash is computed of text on the object.

21. The system of claim 14 wherein the copy detection watermark and the authentication watermark are the same.

22. The system of claim 14 wherein the copy detection watermark comprises one or more watermarks that degrade in response to a reproduction operation on the printed object in a manner that is detectable in a decoding of the one or more watermarks from a reproduced version of the printed object.

23. The system of claim 14 wherein the message includes bearer information that is compared with information provided by the bearer to authenticate the bearer of the printed object.

24. The system of claim 14 wherein the message includes information that is compared with other information derived by machine from the object to authenticate the object.

25. The system of claim 14 wherein the message is associated with a monetary value for the printed object.

26. The system of claim 14 wherein the verification module checks the message associated with the printed object to determine whether the printed object is valid for a particular action.

27. The system of claim 26 wherein the printed object is a ticket or pass and the particular action is entry to an event or access to a vehicle.

28. The system of claim 14 wherein the message includes a time stamp that is used to determine whether validity of the printed object has expired.

29. A system for creating a printed object comprising:

a watermark encoder for encoding a watermark in an image to be printed on a printed object, wherein the watermark is used to authenticate the printed object; and

a communication application for obtaining an identifier from a identifier database for embedding into a message payload of the watermark and for providing information to be associated with the identifier to an object-identifier association database.

30. The system of claim 29 wherein the watermark is a copy detection watermark that degrades in response to a reproduction operation performed on the printed object.

31. The system of claim 29 wherein the information is user information to authenticate the bearer of the printed object.

32. The system of claim 29 wherein the information is a time stamp that is used to determine whether the printed object has expired.

33. The system of claim 29 wherein the encoder is operable to encode a first watermark that includes the identifier linking the printed object to the object-identifier database, and a second, fragile copy detection watermark for discriminating between an original and a reproduction of the printed object.

Fig. 1

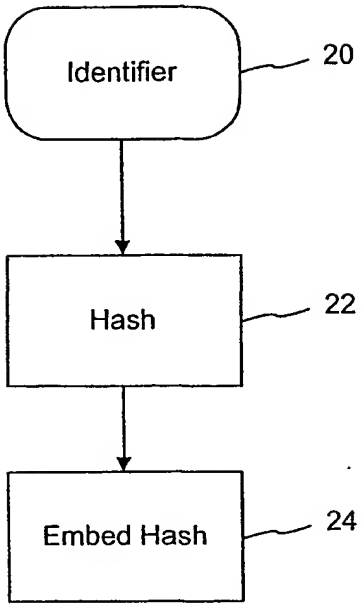

Identifier
20
Hash
22
Embed Hash
24

Fig. 2

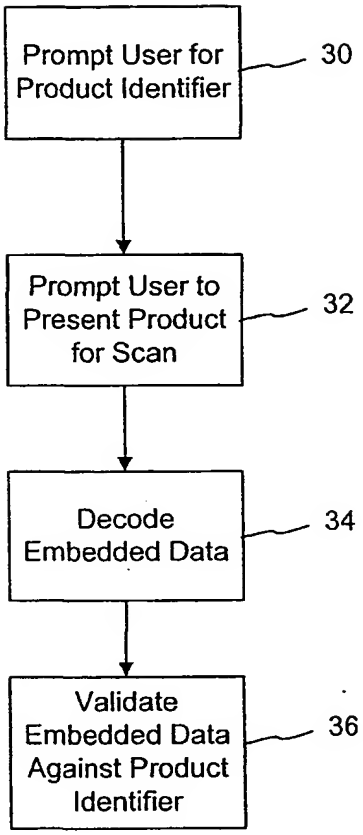
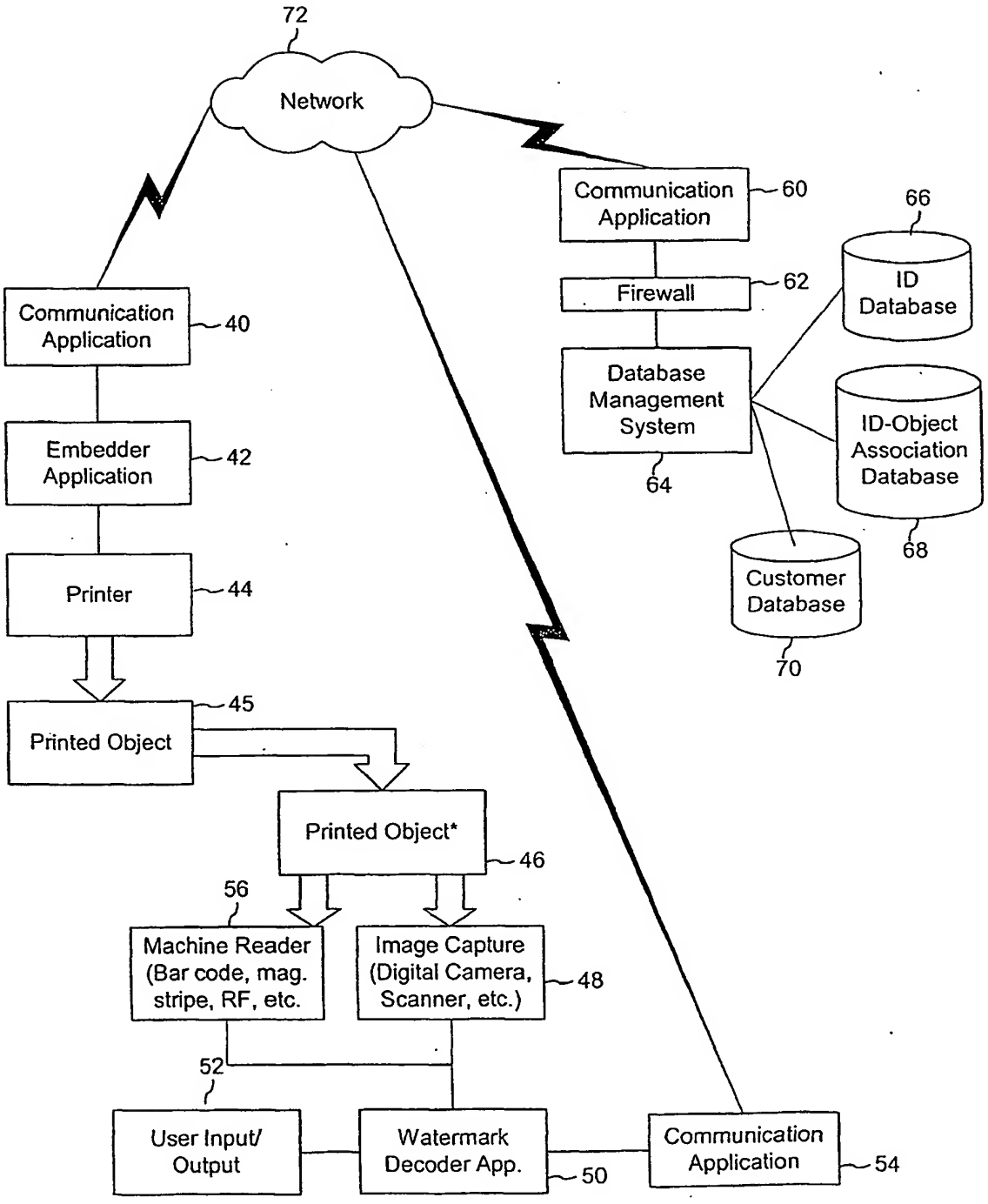

Prompt User for Product Identifier
30
Prompt User to Present Product for Scan
32
Decode Embedded Data
34
Validate Embedded Data Against Product Identifier
36

Fig. 3


72
Network
Communication Application
60
66
ID Database
Firewall
62
Communication Application
40
Database Management System
64
ID-Object Association Database
68
Embedder Application
42
Customer Database
70
Printer
44
Printed Object
45
Printed Object*
46
56
Machine Reader (Bar code, mag. stripe, RF, etc.
Image Capture (Digital Camera, Scanner, etc.)
48
52
User Input/ Output
Watermark Decoder App.
50
Communication Application
54

Application Data Sheet (Multiple Inventors with Representation, Continuity and Priority)
Digimarc Corporation

Inventor Information

Inventor One Given Name::	Osama M.
Family Name::	Alattar
Name Suffix::	
Postal Address Line One::	13935 SW Glastonbury Lane
Postal Address Line Two::	Apt. 242
City of Residence::	Tigard
State or Province of Residence::	OR
Country::	USA
Postal or Zip Code::	97224
Citizenship Country::	USA

Inventor Two Given Name::	Adnan M.
Family Name::	Alattar
Name Suffix::	
Postal Address Line One::	14336 SW Chesterfield Lane
Postal Address Line Two::	
City of Residence::	Tigard
State or Province of Residence::	OR
Country::	USA
Postal or Zip Code::	97224
Citizenship Country::	USA

Correspondence Information

Correspondence Customer Number::	**23735**
Addressee:	Steven W. Stewart
Telephone One::	(503) 469-4800
Fax::	(503) 469-4777
Electronic Mail::	sstewart@digimarc.com

Application Information

Title Line One::	HIERARCHICAL WATERMARK DETECTOR
Total Drawing Sheets::	5
Application Type::	Utility
Docket Number::	P1139L

Representative Information

Representative Customer Number:: **23735**

Continuity Information

This application ::	Claims benefit of
> Application One::	60/610,823
Filing Date::	September 17, 2004
Patent No::	

COMBINED DECLARATION AND POWER OF ATTORNEY FOR PATENT APPLICATION USING AN APPLICATION DATA SHEET (37 CFR 1.76)

As a below named inventor, I/we hereby declare that:

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled HIERARCHICAL WATERMARK DETECTOR, the specification of which

[x] is attached hereto.

[ ] was filed on _____ as Application No. _____.

[ ] was described and claimed in PCT International Application No. _____, filed on _____, and as amended under PCT Article 19 on _____ (if applicable).

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to patentability as defined in Title 37, Code of Federal Regulations, § 1.56. If this is a continuation-in-part application filed under the conditions specified in 35 U.S.C. § 120 which discloses and claims subject matter in addition to that disclosed in the prior copending application, I further acknowledge the duty to disclose material information as defined in 37 CFR § 1.56 which occurred between the filing date of the prior application and the national or PCT international filing date of the continuation-in-part application.

I hereby appoint practitioners at **CUSTOMER NUMBER 23735** (William Y. Conwell, Joel R. Meyer, Thomas M. Horgan and Steven W. Stewart) to prosecute this application, to represent me in filing and prosecuting corresponding international applications, and to transact all business in the Patent and Trademark Office connected therewith:

Address all correspondence and telephone calls to Steven W. Stewart.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

FULL NAME OF INVENTOR(S)	
Inventor one: Osama M. Alattar	Signature: _____
Date: _____	Citizen of: United States
FULL NAME OF INVENTOR(S)	
Inventor two: Adnan M. Alattar	Signature: _____
Date: _____	Citizen of: United States